

## CLAIMS

1/ A method of making secure the transmission of a message Prgm from an emitter device E to a receiver device R, the method being characterized in that:

5       - the message Prgm is subdivided into  $n$  elementary units I, where  $n$  is a number greater than 1;

      - a logical property P is defined in such a manner that for any elementary unit I, the logical property P when applied to an authentic elementary unit I gives a  
10       logical value of the type true;

      - the message Prgm is encrypted by encryption means of the emitter device E using an encryption algorithm having a key Kc so as to obtain an encrypted result Kc(Prgm);

15       - the encrypted result Kc(Prgm) is transmitted by the emitter device E to the receiver device R;

      - the encrypted result Kc(Prgm) is decrypted by the receiver device R using a decryption algorithm having a secret key Kd so as to obtain a decrypted result  
20       Kd(Kc(Prgm));

      - the decrypted result Kd(Kc(Prgm)) is subdivided into elementary units I;

      - the logical property P is applied to the elementary units I so as to obtain, for each unit, a  
25       logical value of the type true or of the type false; and

      - the message Prgm is considered as being authentic and uncorrupted providing the logical value of each unit is of the type true.

a 30       2/ A method according to <sup>claim 1</sup> ~~the preceding claim~~, characterized in that the message Prgm is a computer program suitable for being executed and/or interpreted by the receiver device R.

35       3/ A method according to <sup>claim 1</sup> ~~the preceding claim~~, characterized in that the elementary units are instructions of the program Prgm.

*claim 1*

4/ A method according to ~~claim 2 or 3~~, characterized in that the property P as applied to an elementary unit I gives a logical value of the type true whenever the elementary unit I is executable and/or interpretable.

*claim 1*

5/ A method according to ~~claim 2, 3, or 4~~, characterized in that the property P as applied to an elementary unit I gives a logical value of the type false whenever the elementary unit I is not executable and/or interpretable.

*claim 4*

6/ A method according to ~~any preceding claim~~, characterized in that the receiver device R is a portable object having a memory, of the smart card type.

*claim 1*

7/ A method according to ~~any one of claims 1 to 5~~, characterized in that the receiver device R includes a portable object having a memory, of the smart card type.

8/ A method according to claim 6, characterized in that the portable object having a memory is a subscriber identity module (SIM).

*claim 7*

9/ A method according to ~~any preceding claim~~, characterized in that the message Prgm is written in a high level interpreted language.

10/ A method according to claim ~~9~~, characterized in that the high level language is the Java language.

11/ A method according to claim ~~9 or 10~~, characterized in that the computer program is made up of a set of precompiled instructions.

*claim 11*

12/ A method according to ~~any preceding claim~~, characterized in that the message Prgm is encrypted as a continuous flow or in chained-together blocks.

*claim 1*  
13/ A method according to ~~any preceding claim~~,  
characterized in that the message Prgm is encrypted in  
blocks, and in that the blocks of the encrypted message  
5 Prgm are permuted.

*1*  
14/ A method according to ~~claim 13~~, characterized in that  
one of the permuted blocks is a starting block or an  
end block of the message Prgm.

*claim 1*  
15/ A method according to ~~any one of claims 1 to 12~~,  
characterized in that the result Kc(Prgm) is decrypted in  
blocks, each encrypted block giving rise to a decrypted  
block which occupies the same space as the encrypted  
15 block.

*claim 1*  
16/ A method according to ~~any preceding claim~~,  
characterized in that the encryption and decryption  
algorithms make use of a random number transmitted by the  
20 emitter device E to the receiver device R.

*claim 1*  
17/ A method according to ~~any preceding claim~~,  
characterized in that the message Prgm is recorded, after  
verification, in a non-volatile memory of the receiver  
25 device R.